RECEIVED
CENTRAL FAX CENTER
NOV 30 2006

PATTON BOGGS LLP
ATTORNEYS AT LAW

1660 Lincoln Street, Suite 2050
Denver CO 80264
(303) 830-1776

Facsimile: (303) 894-9239

FAX TRANSMISSION

DATE:	November 30, 2006
PTO IDENTIFIER:	**Application Number** 10/028,004-Conf. #2388 **Patent Number**
Inventor:	Robert R. Gilman et al.
MESSAGE TO:	MS Appeal Brief – Patents (USPTO)
FAX NUMBER:	(571) 273-8300
FROM:	PATTON BOGGS LLP James M. Graziano
PHONE:	303-830-1776
Attorney Dkt. #:	013217.0177PTUS (401043-A-01-US)
PAGES (Including Cover Sheet):	10
CONTENTS:	Certificate of Transmission (1 page) Appellants' Reply Brief (8 pages)

If your receipt of this transmission is in error, please notify this firm immediately by collect call to sender at 303-830-1776 and send the original transmission to us by return mail at the address below.

This transmission is intended for the sole use of the individual and entity to whom it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. You are hereby notified that any dissemination, distribution or duplication of this transmission by someone other than the intended addressee or its designated agent is strictly prohibited.

PATTON BOGGS LLP
1660 Lincoln Street, Suite 1900, Denver, Colorado 80264
Telephone: (303) 830-1776 **Facsimile:** (303) 894-9239

245549

PTO/SB/97 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U. S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application No. (if known): 10/028,004

Attorney Docket No.: 013217.0177PTUS
(401043-A-01-US)

Certificate of Transmission under 37 CFR 1.8

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office.

on November 30, 2006
Date

Elaine C. VonSpreckelsen
Signature

Elaine C. VonSpreckelsen
Typed or printed name of person signing Certificate

N/A
Registration Number, if applicable

(303) 894-6163
Telephone Number

Note: Each paper must have its own certificate of transmission, or this certificate must identify each submitted paper.

Appellants' Reply Brief (8 pages)

245546

RECEIVED
CENTRAL FAX CENTER

NOV 30 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
ON APPEAL BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Patent Application Serial No. 10/028004	Confirmation No.: 2388
Filing Date: December 21, 2001	Art Unit: 2134
For: Secure Data Authentication Apparatus	Examiner: T.M. Szymanski
	Docket No.: 013217.0177PTUS (401043-A-01-US)
Inventors: Robert R. Gilman, Richard L. Robinson, and Douglas A. Spencer	

MAIL STOP APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Dear Sir:

APPELLANTS' REPLY BRIEF

I. APPELLANTS' IDENTIFICATION OF AN ISSUE NOT CLEARLY ADDRESSED IN PRIOR COMMUNICATIONS

In Paragraph 10 of the Examiner's Answer, the Examiner affirms that the Ho Patent is cited to show the teaching in the prior art of an owner key, which is an element absent from the cited Chang Patent, yet recited in Appellants' claims. However, the Examiner, in rejecting Appellants' claims, confuses three independent issues (disclosure, obviousness, and motivation to combine) in his rejections and associated comments. For example, in Paragraph 10 of the Examiner's Answer:

> The applicant has attempted to characterize the Ho reference as teaching against the combination, but it clearly provides the same motivation as the Chang reference of verifying the authenticity of a document against tampering and piracy ....

The existence of a prior art reference that teaches an owner key is irrelevant if this reference fails to address the same problem that is addressed by Appellants' claims or the teachings of the Chang Patent.

It is acknowledged by all parties that, on a global level, both the Chang and Ho Patents are directed to computer software security systems. However, this vague nexus is insufficient to support a claim of motivation to combine the teachings of these two references to anticipate Appellants' claims absent some more specific details. In fact, Appellants' claims are not directed to only "verifying the authenticity of a document against tampering and piracy," but also are directed to simultaneously ensuring that a program purchased to execute on a specific processor runs on only that processor. The Chang Patent is directed to guaranteeing the authenticity of the program, while the motivation of the Ho Patent is protecting Internet Appliances from unauthorized copying. Thus, the cited Chang and Ho Patents address different security concerns, and the motivation issue for determining obviousness of Appellants' claims is whether it is obvious to modify Chang with the teachings of Ho to reconstruct Appellants' claimed invention, not whether both references are simply in the same field of art.

II. BRIEF SUMMARY OF THE PRIOR ART TEACHINGS

The Chang Patent is directed to a system that only determines program authenticity, independent of the computer on which the program runs. The Chang Patent generates a message digest of a program and encrypts this message digest into a passport which is transmitted to the recipient along with the program. The recipient of the program then runs a decrypt process to reconstruct the encrypted message digest, and if the reconstructed message digest fails to match the original message digest, then the program is not an authorized program. There is no concern about which computer runs the program. In fact, the Chang Patent is devoid of even a hint of a program being authorized to run only on a specific computer, and the identity of the computer which runs the program of the Chang Patent is irrelevant.

On the opposite end of the spectrum, the Ho Patent teaches storing a computer-specific engraved signature in the computer memory, then regenerating the computer-specific engraved signature from the computer's Network Interface Card prior to running the program, to verify that the computer memory has not been disassociated from the computer. However, the Ho Patent fails to integrate the program into this

process to verify that the program is an authorized copy of the program and run only on the destination computer. The Ho Patent is devoid of even a hint that the program can be used with a computer specific owner key to ensure that the program is run on only the single computer that is authorized to run this instance of the program.

Thus, the Chang Patent teaches encrypt-decrypt of a passport that is delivered with the program to ensure authenticity of the program, independent of the identity of the computer that executes the program, while the Ho Patent teaches regenerating a computer-specific engraved signature to ensure that the computer memory has not been disassociated from the computer, regardless of the authenticity of the program or the contents of the program.

Appellants' system differs from these processes taught by these references, but uses the program contents in conjunction with an owner key that uniquely identifies the computer to match the computer to the computer-specific copy of the program to ensure that the computer is authorized to run this specific copy of the program. The program distributor computes a first signature by hashing at least part of the program and using the owner key that is specific to the recipient computer to encrypt this hash value. The program owner then transmits the program and the first signature to the recipient computer, which computes a second signature by hashing at least part of the program and using the owner key that is specific to the recipient computer to encrypt this hash value. If both computed signatures match, then the program is an authentic program and is also authorized to run on only the destination computer. The benefit of creating a unique owner-specific source signature to append to the installation software is to prevent unauthorized individuals, who may obtain the software file in an unscrambled form, from using the software file without authorization. Appellants' system validates the authenticity of the program and concurrently determines whether the recipient computer is authorized to execute this copy of the program.

RECEIVED
CENTRAL FAX CENTER
NOV 30 2006

III. APPELLANTS' INDEPENDENT CLAIM 1

As an example of the independent claims presented in this application, independent claim 1 corresponds to the above-noted summary of Appellants' invention, where Appellants' system validates the authenticity of the program and concurrently determines whether the recipient computer is authorized to execute this copy of the program:

> 1. (Previously presented) A secure data authentication apparatus 150 to authenticate a software file 300, the software file having a first signature 340 appended to the software file 300, for use on a computer system 100, wherein said computer system 100 is assigned an owner key 210 that is unique to said computer system 100, said first signature 340 comprising a source hash value 230 that is computed by processing at least some of said software file 300 using a selected hash function, which source hash value 230 is encrypted using said owner key 210 to produce said first signature 340, the apparatus comprising:
>
> a secure processing device 150 within the computer system 100 to receive the software file 300 and hash the software file 300 using said selected hash function to produce a first hash value 240 (Page 14, Lines 11 – 19); and
>
> a first key 272 located within the secure processing device 150, which first key 272 comprises said owner key 210 wherein the secure processing device 150 encrypts the first hash value 240 with the first key 272 to generate a second signature 430 and compares the first signature 340 with the second signature 430, and if the first signature 340 matches the second signature 430, the computer system 100 accepts the software file 300 as being authenticated (Page 16, Line 3 – Page 17, Line 7).

IV. APPELLANTS' DETAILED CHARACTERIZATION OF THE REFERENCES

The cited Chang Patent teaches that, to protect a source code file, a software application writer's private key, along with an application writer's license, is provided to

a first computer. The application writer's license includes identifying information, such as the application writer's name, as well as the application writer's public key. A compiler program executed by the first computer compiles the source code into binary code and computes a message digest for the binary code. The first computer then encrypts the message digest using the application writer's private key, such that the encrypted message digest is defined as a digital "signature" of the application writer. A software passport then is generated which includes the application writer's digital signature, the application writer's license, and the binary code. A user, upon receipt of the software passport, loads the passport into a computer, and the user's computer computes a second message digest for the software passport and compares it to the first message digest, such that if the first and second message digests are not equal, the software passport is also rejected by the user's computer and the code is not executed.

The Ho Patent teaches:

> A method and an apparatus for using an encrypted unique digital signature ("engraved signature") as a uniquely definable signature to control the use or execution of software in a computer system. The computer system has a Network Interface Card ("NIC") with a Media Access Control ("MAC") address. On start up, the engraved signature is retrieved from the persistent storage medium of the computer system and the MAC address is retrieved from the NIC. A computed encrypted signature is generated using the MAC address. Where the computed encrypted signature does not match the engraved signature, the execution of the software is halted. **(Abstract)**

However, the Ho Patent is limited to a self-contained storage medium and a network interface card, as noted in paragraphs [0008] – [0010]:

> **[0008]** The problem of software piracy is acute with a particular class of computer systems: Internet Appliances. An Internet Appliance is generally a computer system that performs some predetermined functions while

connected to the Internet. The Internet Appliances typically consist of computer hardware with embedded software. The hardware includes a storage medium and a network interface card.

[0009] Software embedded in an Internet Appliance tends to be compact. It is not uncommon to store the entire system software in a storage medium that has only a few megabytes of capacity. This type of storage medium is usually small and very portable (such as CompactFlash and SIM cards). Because of wide adaptation and portability of such media, digital content inside such mediums can be illegally duplicated very easily.

[0010] It is therefore an aspect of an object of the present invention to provide a method and an apparatus for protecting the embedded software in computer systems, such as Internet Appliances, against unauthorized use, while being relatively cost-effective to deploy.

The Ho Patent, in defining the preferred embodiment, notes that it is impractical to execute a unique compilation of the software for each end user computer, and clearly indicates that this system is predicated on the "restricted entitlement" mode of operation, which is defined in the Background of the Invention as:

> **[0005]** Restricted entitlement means that the software contains some means to limit itself to run only on the computer system for which it is authorized. A common restriction method is to encode hardware specific information in the computer system so that the software can verify the information at system startup. Another method is to make the software unique for every computer system. This entails unique compilation of the software for each distribution, which is a very costly operation.

V. APPELLANTS' INVENTION

In contrast to the teachings of the cited references, Appellants' secure data authentication apparatus makes use of a file transmission protocol where "the software file having a first signature appended to the software file", and the user's "computer system is assigned an owner key that is unique to said computer system." The hash value is computed "by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature." Furthermore, Appellants' secure data authentication apparatus includes "a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature." When the user's computer receives the software file and the associated digital signature, it can recompute the digital signature using an owner's key that is specific to the target telephone switching system and compare it to the received digital signature. Thus, Appellants' independent claim 1 recites structure that is not shown or suggested by the cited references; Appellants' system validates the authenticity of the program and concurrently determines whether the recipient computer is authorized to execute this copy of the program.

VI. SUMMARY

Appellants believe that claims 1 – 15 and 18 are allowable under 35 U.S.C. §103(a) over the cited references for the reasons articulated above.

Appellants respectfully request a Notice of Allowance in this application in light of the arguments set forth herein. The undersigned attorney requests Examiner Szymanski to telephone if a conversation could expedite the prosecution of this application. Appellants authorize the Commissioner to charge any additionally required

payment of fees to our Deposit Account No. 50-1848, under Order No. 013217.0177PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: 11/30/06

By: _____
James M. Graziano
Registration No.: 28,300
(303) 830-1776

(303) 894-9239 (Fax)
Attorney for Appellants

Customer No. 24283